Category	Index Code Page
Information Technology	
Reference	**Date**
	September 23, 2002
Issued by	
Department of Information Technology	
Subject	
Internet Policy & Guidelines	

I. Background

The City and County of Honolulu provides INTERNET access capability to its employees as a business tool to help them gain greater insight to emerging technologies; to promote creative ideas on increasing revenues and reducing cost; to provide access and sharing of information for more informed decision-making; to effectively communicate with other INTERNET users around the world; and to provide research capabilities for their normal job.

II. Internet Security

Although the INTERNET has provided opportunity for information exchange among millions of users, it is unsecured and unregulated. It provides opportunities for unauthorized access to other connecting networks, illegal penetration of networks by "hackers", fraudulent data manipulation, introduction of computer viruses, and many other security-related problems. Therefore, it is mandatory that each employee accessing the INTERNET take proper precautions to protect the City and County of Honolulu's network and data from unauthorized access and tampering.

The City allows access and services to selected functions on the INTERNET which have minimal impact on network security. These services include, but not limited to:

- World Wide Web
- E-mail
- Network News
- File Transfer Protocol (FTP)
- Telnet
- Ping
- Domain Name Services

III. Internet Access Through Service Providers

Access to the INTERNET via a commercial service provider must go through the City's local area network (LAN) modems if the workstation is connected to the City's network or access must made via a stand-alone workstation.

IV. General Guidelines

A. INTERNET Access

1. City employees who have been authorized by their department to utilize INTERNET services are allowed to participate in the City's INTERNET offering.

2. All information created, sent or received via the e-mail system, network or INTERNET is the property of the City. Employees should not have any expectation of privacy regarding such information. However, the requesting department Director must submit a written request with proper justification to the DIT and DHR Director for approval in order to access such information.

3. Access to the INTERNET from the City's network shall be via DIT approved software. Agencies should not use other web-browsing software.

4. All data sets, files, software/shareware, or any other material downloaded from the INTERNET must be scanned for possible viruses prior to its use. Users should have a thorough knowledge of the source of all materials before its use. Be aware that new viruses are being created and oftentimes may not be detected by virus scanners. Therefore, users should exercise extreme caution before utilizing INTERNET files.

B. INTERNET Usage

1. All INTERNET usage shall be used for official City business only.

2. The following are examples of INTERNET uses that are not acceptable:
   - Commercial for-profit purposes
   - Product advertisement or political lobbying (other than for City purposes)
   - Engaging in disruptive activities such as software/information destruction or unauthorized changes to files
   - Virus uploading, downloading, creation and/or propagation
   - Fraudulent, harassing, offensive, obscene or pornographic messages and/or materials are not to be sent, viewed, downloaded, printed, requested or stored
   - Game-playing
   - Installing, copying, or distributing any copyrighted material in violation of copyright laws
   - Gambling or engaging in any other activity in violation of

local, state or federal law

- Uses that jeopardize the security of the City's Network or other networks on the INTERNET (For example, don't disclose or share your password with others and don't impersonate another)
- Suggesting to other associates that they view, download, or seek materials, files, information, software or other content that may be offensive, defamatory, misleading, infringing or illegal

3. Any confidential information being transmitted over the INTERNET should be encrypted.

4. Every City employee is responsible for ensuring that INTERNET services will be used in an efficient, ethical, and lawful manner.

C. INTERNET Electronic Mail (E-mail) and Usenet Posting

1. INTERNET E-mail is not to be archived within the City's E-mail system. Messages to be kept must be either printed or saved to a removable disk file outside of the system.

2. To help prevent against viruses, the email system does not allow .exe, .com, .vbs and .dll attachments from/to the INTERNET.

D. INTERNET Training

1. Each City agency will be responsible for seeking adequate training for its authorized INTERNET users.
   - Usage and how-to technical training are available for a fee at the community colleges and commercial training centers
   - INTERNET's World Wide Web provides documentation (at no charge) describing the many functions of INTERNET
   - Books and videos are available commercially on INTERNET ranging from basic concepts to advanced techniques

2. DIT will provide procedures on how to access INTERNET on the City network and basic concepts on available facilities on INTERNET.

V. Logging and Monitoring

A. The City reserves the right to log all traffic to/from the INTERNET including web and mail.

B. With proper approval and authorization of the DIT and DHR Director, the City reserves the right to, at any time and without notice, access, read and review, monitor, and copy all messages and files on its computer system, without the employee's consent, to satisfy a business purpose or satisfy a legal obligation. The requesting department Director must submit a written request with proper justification to the DIT and DHR Director for approval.

C. The City reserves the right to provide appropriate logs to authorized City users for business purposes.

D. When it believes necessary, the City may disclose files, text or images to law enforcement or other third parties without the employee's consent to satisfy an important business purpose or satisfy a legal obligation.

E. It is a violation of City policy for any employee, including system administrators and supervisors, to monitor the INTERNET usage of others with no substantial business purpose for obtaining the information.

VI. Duties and Responsibilities

A. Department of Information Technology (DIT) is responsible to:

1. Budget for, provide, and maintain the City's physical connection to INTERNET.

2. Provide the hardware and software tools necessary to safeguard the City's information from possible unauthorized access or data destruction resulting INTERNET use.

3. Provide the central software, guidelines, and procedures for accessing the INTERNET.

4. Advise and assist City users in installing the software to access INTERNET on request.

5. Provide training on how to sign on to INTERNET in the City's network.

B. City Agencies are responsible to:

1. Assess the need for INTERNET access requests by its employees and provide DIT with the names of authorized departmental users.

2. Assess the need for the type of access required and limit access to website appropriately.

3. Provide all authorized departmental users with the necessary hardware and software to efficiently utilize the City's INTERNET services.

4. Establish departmental policy and authorization procedures for INTERNET use.

5. Maintain a list of authorized departmental INTERNET users.

6. Assure that users receive adequate training on INTERNET use.

7. Ensure departmental use of the INTERNET is in compliance with established City and departmental policy and guidelines.

8. Discipline users consistent with personnel polices and procedures for violations of the City's information technology security guidelines.

C. Users are responsible to:

1. Adhere to all City and departmental INTERNET policies and guidelines.

2. Assume individual responsibility for safeguarding the City's network, equipment, and information from unauthorized use.

3. Assume responsibility for the accuracy, validity, and source of all information obtained via the INTERNET. Be aware that INTERNET information is neither controlled nor verified.

4. Refrain from circumventing established controls.

VII. Compliance/Non-Compliance

A. By accessing the INTERNET, you are agreeing not only to follow the rules in this Policy, but also you are agreeing that any misuse of access to the Network or the INTERNET should be reported to your supervisor or department head. Misuse means any violations of this Policy, or any other use that, while not included in this Policy, has the effect of harming another or another's property.

B. Non-compliance with the City's INTERNET policies, guidelines or procedures may result in the revocation of INTERNET privileges and/or other appropriate disciplinary action, including reprimand, suspension, termination of employment, or, if warranted, civil or criminal prosecution.